White Paper

LDRPS and TERMx:

How Organizations Can Effectively Manage Operational Risks

Summary

Even before Sept. 11, operational risk was a hot topic in corporate boardrooms. Since then, managing operational risk is even more of a top priority.

In a recent survey jointly conducted by Strohl Systems and *Contingency Planning & Management* magazine, 41 percent of the business continuity planning professionals responding to the survey thought Sept. 11 would most likely cause an increase in physical security for their organization. In addition, 24 percent though it would most likely cause an increase in information security. Both of these items fall under operational risk management.

Operational risk is "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events."[1] Basically operational risk includes all risks outside of financial risks such as technology, legal, political, personnel, etc. Operational risk management is a relatively new, yet valuable, concept. It varies from risk management because risks are monitored and mitigated in real-time. Software tools are needed to track, monitor, and effect the changes.

Strohl Systems has a solution that can ensure help organizations effectively manage operational risk. Strohl's industry leading business continuity planning software, LDRPS[2], used in conjunction with Strohl's Total Enterprise Risk Management (TERMx) methodology can give enterprises the edge they need.

TERMx and LDRPS offer the ability to:

- Record, categorize, rate, and score every type of operational risk in a self-contained risk register, and link these risks dynamically to specific business units and processes;
- Allocate accountability and responsibility for the management and mitigation of each risk and associated expenditures right down to an individual;
- Score every risk or group of risks and use a unique algorithm to determine "effectiveness" scoring for the mitigation activities implemented. This enables true risk management by objective;
- Monitor the status, effectiveness and costs/expenditures of all mitigation activities either by individual risk, by department, by region, or across the entire enterprise. Because TERMx is driven by a Web-based engine, risk managers or executive managers have the ability to monitor their company's risk status on a real-time basis.
- Provide multiple, executive viewpoint reports that give complete summaries of the organization's risk profile;
- Demonstrate an organization's adherence to "sound practices for the management and supervision of operational risk."

The specifics of the TERMx methodology and how it can be used with LDRPS to effectively manage operational risks are outlined in the following pages.

How TERMx Works

TERMx is a new risk management methodology that works in conjunction with LDRPS. Strohl's risk management experts created its proprietary system to track, rate, and report on the status of an organization's risk management program.

Strohl consultants are available to walk organizations through the entire process from project initiation, to data gathering and analysis, to reporting and finally to implementation. Strohl's experts can run the whole project or just get you started and provide guidance along the way.

The first step in an effective risk management program is to document the existing risks. Once risks are identified (either by internal sources or by Strohl's experts) they are recorded into an LDRPS risk register. These risks are then condensed into specific Risk Control Objective (RCO) categories, which are as follows:

- Physical (access control, identification);
- Logical (information security, computer network control, data backups);
- Operational (process dependencies, process flows);
- Procedural (standard operating procedures, emergency operating procedures);
- Supervisory (authorizations, monitoring);
- Environmental (air quality, fire prevention, flood detection).

For example, it is noted that ABC Corporation lacks a standard system for access controls and does not have an appropriate discipline for backup and off site storage of data. The RCO would then become, "To implement a corporate-wide information protection solution within ABC Company to conform to recognized industry data protection standards and best practices." In the LDRPS risk register, this RCO would be added to the Logical Controls risk category.

In order to achieve an RCO, certain tasks will need to be performed. These tasks, termed Risk Mitigation Activities (RMA), must be completed to reduce or eliminate the identified risk.

LDRPS and TERMx:

How Organizations Can Effectively Manage Operational Risks

(c o n t i n u e d)

Each RMA is also recorded in the risk register and assigned to the relevant objective. RCOs may have many tasks assigned to them. Resources and personnel are assigned to each RMA and risk managers can adjust the resources based on scope changes, timelines, and budgetary needs.

Using the previous example, ABC Corporation may identify the following RMAs that need to be completed to effectively reduce or eliminate the risk posed by the lack of a standard data protection system.

1. Commission a data classification and inventory exercise to construct a vital records register. Utilize this register to map firewall rules and to determine data protection confidentiality rules.
2. Perform full systems security audit on all mainframe, mid-size and server system, and document and validate all access rights.
3. Develop and implement a data backup policy that dictates the frequency, format, retention and security parameters for back-up images.
4. Conduct a review of all end-user laptop / PC configurations to determine current virus-proofing capabilities and deficiencies.

Facilities Management (Health and Safety Compliance) **Implement, Manage and Control all Health & Safety Act Requirements**		**Priority 1**	**Impact Severity High**
The Health & Safety 2001 Audit Identified Unacceptable H&S Risks at the Crosby Court Facility. Regulators have given ABC until 30 August 2002 to rectify specific exposures.		RMA Effectiveness Rating **5**	
New Risk	Design, implement and manage a preventative maintenance program for ABC Crosby Court.		
10% completed	Revise all building evacuation plans at Crosby Court. Appoint and train (bi-annually) two fire and evacuation wardens per floor.	RMA Effectiveness Rating **5**	
50% completed	Develop and submit for tender RFP for the safe removal of asbestos in ceilings at Crosby Court.	RMA Effectiveness Rating **5**	
60% completed	Implement a method for recording physically disabled staff members at ABC Corporation and implement appropriate evacuation procedures for each disabled employee. Test procedures for effectiveness.	RMA Effectiveness Rating **4**	
Not Started	Conduct monthly fire and evacuation tests.	RMA Effectiveness Rating **4**	
Not Started	Ensure that 15% of all ABC staff members are certified in first aide by 30 June 2002. Implement a training program to ensure re-certification process.	RMA Effectiveness Rating **4**	
Completed	Conduct ABC Health & Safety Monthly Inspection	RMA Effectiveness Rating **3**	
Accepted Risk	Approve the Health and Safety department as the single entity for control and management of hazardous chemicals (acquisition, monitoring, secure storage, disposal, etc.)	RMA Effectiveness Rating **2**	
Percentage of Risk Mitigation Activities Completed **13%**		**Mitigation Activity Effectiveness Rating:** **16%**	

Figure 1: Sample Risk Control Objectives Summary Report for ABC Corporation

LDRPS and TERMx:

How Organizations Can Effectively Manage Operational Risks

(c o n t i n u e d)

Determine update frequency, signature file refresh procedures, and false/positive trend analysis.

Administrators score the effectiveness each RMA will have on reducing the organization's overall risk. The RMAs are scored on a scale of 1 to 5 (five being the most effective). Risk scoring prioritizes the implementation of RCOs and allows executive management to effectively set implementation objectives and timelines.

All of the risks, risk categories, RCOs, and RMAs are tracked and managed in LDRPS. As work on the RMAs progresses, it is entered

Facilities Management (Health and Safety Compliance)

Approved Investment	*Risk Control Objective*		Priority	Impact Severity
$2,000,000	Implement, Manage and Control all Health & Safety Act Requirements		1	High
Mitigation Activity Cost	***Mitigation Activity Description***			***RMA Effectiveness Rating***
$1,000,000	Develop and submit for tender RFP for the safe removal of asbestos in ceilings at Crosby Court.	50% completed		5
$20,000	Revise all building evacuation plans at Crosby Court. Appoint and train (bi-annually) two fire and evacuation wardens per floor.	10% completed		5
$5,000	Design, implement and manage a preventative maintenance program for ABC Crosby Court.	New Risk		5
$5,000	Ensure that 15% of all ABC staff members are certified in first aide by 30 June 2002. Implement a training program to ensure re-certification process.	Not Started		4
$2,000	Implement a method for recording physically disabled staff members at ABC Corporation and implement appropriate evacuation procedures for each disabled employee. Test procedures for effectiveness.	60% completed		4
$2,000	Conduct monthly fire and evacuation tests.	Not Started		4
$1,000	Conduct ABC Health & Safety Monthly Inspection	Completed		3
$2,500	Approve the Health and Safety department as the single entity for control and management of hazardous chemicals (acquisition, monitoring, secure storage, disposal, etc.)	Accepted Risk		2

Mitigation Activity Cost Total	Approved Investment Remaining
$1,037,500	$962,500

% of Risk Mitigation Activities Completed:	Total Cost of Mitigation Activities:	Total Investment Remaining:	Mitigation Activity Effectiveness Rating:
25%	$1,037,500	$962,500	16%

Figure 2: Sample Risk Mitigation Investment Report for ABC Corporation.

LDRPS and TERMx:

How Organizations Can Effectively Manage Operational Risks

(c o n t i n u e d)

into the system. For example, when an RMA is halfway completed, the supervisor responsible for that task enters into LDRPS that it is 50 percent complete. Supervisors can track the status of each RMA as it progresses and reassign resources as needed.

Using a proprietary algorithm, that takes into account the amount of work completed and the criticality score of each RMA, TERMx and LDRPS calculate the effectiveness of the risk management program as it is ongoing. Executives, insurance regulators, or auditors can view the progress of the risk management program in real time.

To put it simply, TERMx and LDRPS provide a "project status report" for the ongoing risk management program and provide effective risk management reporting and monitoring.

When used with LDRPS Web Server version, TERMx comes pre-packaged with many useful reports. These reports include:

Risk Control Objectives Summary Report (Figure 1)

- An executive-level viewpoint of all identified risks, their description, assigned risk category, priority rating, and impact severity.
- Details of the RMAs that must be executed or implemented in order to mitigate an identified risk.
- Overall progress of RMAs (i.e. the percent of RMAs completed).
- Status of each RMA.
- Overall benefit derived from completed RMAs (i.e. the percent of identified risks that have been mitigated to an acceptable level).

Risk Mitigation Activity Prioritization Report

This report provides the order in which each RMA should be executed or implemented to achieve the best return on investment.

Risk Mitigation Investment Report (Figure 2)

This report provides the overall risk management budget status and consumption of this approved investment by each RMA.

Conclusion

Using TERMx in conjunction with LDRPS enables organizations to effectively manage and control their operational risks.

TERMx provides a standardized process to track, monitor, and score risks in any organization. Risk managers can now effect changes based on real-time information. In addition, senior executives can view the status, budget, and success of the program in real time.

For more information about TERMx and how it can assist your organization, contact Strohl Systems at 1-800-634-2016 or visit www.strohlsystems.com.

End Notes

[1] *Definition is according to the Bank for International Settlements (BIS). More information about the BIS and the organization's opinions on operational risk management can be found at* www.bis.org.

[2] *For a complete list of features of Strohl's business continuity planning software, LDRPS visit* www.strohlsystems.com/Software/LDRPS.